Notice of Allowability	Application No.	Applicant(s)	
	09/733,014	WRAY ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/7/2005*.

2. ☒ The allowed claim(s) is/are *1,2,4,5,7,9,10,13,15,16,19 and 20*.

3. ☒ The drawings filed on *23 July 2001* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

2. Applicant's submission filed on April 22, 2005 has been entered and made of record.

Response to Arguments

Allowable Subject Matter

3. Claims 1, 2, 4, 5, 7, 9, 10, 13, 15, 16, 19 and 20 are allowed.

4. The following is an examiner's statement of reasons for allowance: The Admitted prior art Aziz et al. U.S. Patent 6,643,701, hereafter "Aziz", disclose a system and method for providing secure communication between a first computer and a second computer wherein the first computer passes first attribute justification (request for

service by authenticating one another using certificate) to the proxy (relay server) and receives the authentication token such as passwords, certificates and private keys and second computer (relay or proxy server) passes to said peer security entity a third indication (the period based on an elapse of a predetermined time) and to receive second attribute justifications in the form of public/private key pair, sever certificate.

However, the admitted prior art does not disclose, teach or suggest "to pass to said peer security entity a first indication in the form of explicit information about what services are required by the local application entity, to receive back from said peer security entity a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services, to select on the basis of said second indication first attribute justifications in the form of one or more certificates from a set of available attribute justifications, and to pass the selected first attribute justifications" and "the first message passing from the local security entity to said peer security entity and including said first and third indications, the second message passing from the peer security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said peer security entity and including said first attribute justifications".

The present invention provides both sensitive and non-sensitive services requiring high or low security attribute justifications allows a local application to pass to

peer security entity a first indication in the form of explicit information about what services are required by the local application entity, to receive back from said peer security entity a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services. Thus, the present invention further provides flexibility with security attribute justifications to a local application entity to gain access to both sensitive and non-sensitive services provided by the peer security entity.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Robert Popa, registration number 43,010 and Laurent Lushinchi, on June 15, 2005.

IN THE CLAIMS:

1. (Amended) A system with a local application entity and communications means by which the local application entity can communicate with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a transport-independent, session-level security entity logically positioned above the transport entity and visible to the local application entity, the security entity being operative to set up secure communication sessions with peer security entities in other systems and comprising:

key-exchange handshake means for conducting a handshake with a said peer security entity associated with a particular remote application entity with which said local application entity wishes to communicate, this handshake involving the exchange of key-related data for use in generating session keys; and

secure channel means for enabling messages to be passed between the local application entity and said particular remote application entity with authentication and/or encryption of these messages being effected using the session keys generated from said key-related data whereby to secure these messages in passage between the cooperating security entities;

the handshake means including:

first means, operative in the course of said handshake, to pass to said peer security entity a first indication in the form of explicit information about what services are required by the local application entity, to receive back from said peer security entity a second indication explicitly advising what specific attributes are required of the local application entity by the remote application entity for carrying out said services, to select on the basis of said second indication first attribute justifications in the form of one or more certificates from a set of available attribute justifications, and to pass the selected first attribute justifications to said peer security entity, and

second means, operative in the course of said handshake, to pass to said peer security entity a third indication explicitly advising what specific attributes are required of

the remote application entity by the local application entity, and to receive second attribute justifications, in the form of one or more certificates, from said peer security entity;

wherein said handshake as a three message handshake, the first message passing from the local security entity to said peer security entity and including said first and third indications, the second message passing from the peer security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said peer security entity and including said first attribute justifications.

2. A system according to claim 1, wherein the security entity is capable of establishing multiple concurrent security sessions with another system over a common transport connection set up by the transport entity.

3. (Canceled)

4. A system according to claim 1, further comprising attribute justification means for proving from certificates received from the remote system during said handshake that the remote application has the required attributes.

5. A system according to claim 1, wherein said local application entity is a mediation entity acting on behalf of one or more other application entities.

6. (Canceled)

7. A system according to claim 1, wherein the security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

a session indicator enabling the peer security entity to determine to which security session the PDU relates; and

a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure channel of the security session indicated by said session indicator.

8. (Canceled)

9. A system according to claim 1, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms that will be subsequently used by the secure channel means for the security session concerned.

10. A system according to claim 9, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

11-12 (Canceled)

13. (Amended) A method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport-independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys, the handshake further involving

passing from the local security entity to the remote security entity a first indication in the form of explicit information about what services are required by the local system, passing from the remote security entity to the local security entity a second indication explicitly advising what specific attributes are required of the local system by the remote system for carrying out said services,

selecting on the basis of said second indication first attribute justifications from a set of available attribute justifications and passing from the local security entity to the remote security entity, the selected first attribute justifications in the form of one or more certificates, and

passing from the local security entity to the remote security entity a third indication explicitly advising what specific attributes are required of the remote system by the local system, and passing from the remote security entity to the local security entity second attribute justifications, in the form of one or more certificates;

wherein said handshake is a three message handshake, the first message passing from the local security entity to said remote security entity and including said first and third indications, the second message passing from the remote security entity to the local security entity and including said second indication and said second attribute justifications, and the third message passing from the local security entity to said remote security entity and including said first attribute justifications.

14. (Canceled)

15. A method according to claim 13, wherein in the course of said handshake an authenticated ephemeral key exchange is effected, and a cipher suite is negotiated determining the authentication and/or encryption algorithms to be subsequently used for secure communication between the local and remote systems.

16. A method according to claim 15, wherein said authenticated ephemeral key exchange is a Diffie-Hellman key exchange.

17-18. (Canceled)

19. A method according to claim 13, wherein each security entity formats its communications intended for the remote peer security entity in protocol data units (PDUs) that each include:

a session indicator enabling the peer security entity to determine to which security session the PDU relates; and

a message-type field by which the peer security entity can determine whether the PDU carries handshake-related data or a message being passed over the secure

channel of the security session indicated by said session indicator.

20. (Amended) A method of initiating secure communication between a local and a remote system wherein a security protocol handshake is effected between respective transport-independent, session-level security entities of the local and remote systems during which handshake key-related data is exchanged for use in generating session keys, the handshake further involving:

the local security entity explicitly indicating to the remote security entity the services and specific attributes required of said remote system by the local system,

the remote security entity explicitly indicating to the local security entity the specific attributes that the remote system requires of the local system in respect of said services, and

the exchange of attribute justifications, in the form of certificates, between the security entities, wherein the attribute justifications passed from the local security entity to the remote security entity are chosen from a set of available attributes justifications, on the basis of the explicit indication of the specific attributes that the remote system requires of the local system;

wherein said handshake as a three message handshake, comprising: a first message passing from the local security entity to said remote security entity and indicating the services and attributes required of said remote system by the local system, the second message passing from the remote security entity to the local security entity and indicating the attributes that the remote system requires of the local system in respect of said services, and the second message also including attribute justifications provided by the remote system, and a third message passing from the local security entity to said remote security entity and including attribute justifications provided by the local system.

21-22. (Canceled)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
June 16, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100